CLAIMS

What is claimed is:

1. A method of creating a strong pass phrase, the method comprising:

obtaining a plurality of questions and a plurality of answers corresponding to the plurality of questions; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

2. The method of claim 1, further comprising transmitting the plurality of questions to a remote server.

3. The method of claim 2, further comprising:

obtaining a set of retrieval questions and a set of retrieval answers corresponding to the set of retrieval questions;

combining the set of retrieval answers into a single retrieval pass phrase; and

transmitting the set of retrieval questions and the retrieval pass phrase to the remote server.

4. The method of claim 3, wherein the plurality of questions consists of a plurality of pass phrase questions, the plurality of answers consists of a plurality of pass phrase answers corresponding to the pass phrase questions, the set of retrieval questions consists of a retrieval question, and the set of retrieval answers consists of a retrieval answer corresponding to the retrieval question.

5. The method of claim 1, wherein the plurality of questions are obtained by displaying a plurality of partial questions and obtaining completions to said plurality of partial questions.

6. The method of claim 1, wherein the pass phrase is used to wrap data to be stored in a remote server.

7. A method of providing a pass phrase at a client workstation, the method comprising:

displaying a plurality of entries for entering a plurality of pass phrase answers; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

8. The method of claim 7, further comprising displaying the plurality of pass phrase questions corresponding to a plurality of pass phrase answers pre-stored in a remote server.

9. The method of claim 8, further comprising obtaining the plurality of pass phrase questions from the remote server.

10. The method of claim 9, further comprising providing an option for displaying the plurality of pass phrase questions.

11. The method of claim 10, further comprising requiring a retrieval pass phrase before the remote server will release the plurality of pass phrase questions, wherein the retrieval pass phrase is pre-stored in the remote server and is formed from a set of retrieval answers previously entered by a user.

12. The method of claim 11, further comprising providing an option for displaying a set of retrieval questions which corresponds to the set of retrieval answers and pre-stored in the remote server.

13. The method of claim 12, wherein a user having registered the set of retrieval questions is notified if anyone asks for the set of retrieval questions.

14. The method of claim 12, further comprising displaying the set of retrieval questions.

15. A computer readable medium for use in conjunction with a client workstation and a server for creating a strong pass phrase, the computer readable medium including computer readable instructions encoded thereon for:

obtaining a plurality of questions and a plurality of answers corresponding to the plurality of questions; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

16. The computer readable medium of claim 15, further including computer readable instructions encoded thereon for comprising transmitting the plurality of questions to a remote server.

17. The computer readable medium of claim 16, further including computer readable instructions encoded thereon for:

obtaining a set of retrieval questions and a set of retrieval answers corresponding to the set of retrieval questions;

combining the set of retrieval answers into a single retrieval pass phrase; and

transmitting the set of retrieval questions and the retrieval pass phrase to the remote server.

18. The computer readable medium of claim 17, wherein the plurality of questions consists of a plurality of pass phrase questions, the plurality of answers consists of a plurality of pass phrase answers corresponding to the pass phrase questions, the set of retrieval questions consists of a retrieval question, and the set of retrieval answers consists of a retrieval answer corresponding to the retrieval question.

19. The computer readable medium of claim 15, wherein the plurality of questions are obtained by displaying a plurality of partial questions and obtaining completions to said plurality of partial questions.

20. The computer readable medium of claim 15, wherein the pass phrase is used to wrap data to be stored in a remote server.

21. A computer readable medium for use in conjunction with a client workstation for providing a pass phrase at a client workstation, the computer readable medium including computer readable instructions encoded thereon for:

displaying a plurality of entries for entering a plurality of pass phrase answers; and

combining the plurality of answers into a single pass phrase, wherein the plurality of answers are concatenated together with a fixed random value and a cryptographic hash function is applied to the concatenation.

22. The computer readable medium of claim 21, further including computer readable instructions encoded thereon for displaying the plurality of pass phrase questions corresponding to a plurality of pass phrase answers pre-stored in a remote server.

23. The computer readable medium of claim 22, further including computer readable instructions encoded thereon for obtaining the plurality of pass phrase questions from the remote server.

24. The computer readable medium of claim 23, further including computer readable instructions encoded thereon for providing an option for displaying the plurality of pass phrase questions.

25. The computer readable medium of claim 24, further including computer readable instructions encoded thereon for requiring a retrieval pass phrase before the remote server will release the plurality of pass phrase questions, wherein the retrieval pass phrase is pre-stored in the remote server and is formed from a set of retrieval answers previously entered by a user.

26. The computer readable medium of claim 25, further including computer readable instructions encoded thereon for providing an option for displaying a set of retrieval questions corresponds to the set of retrieval answers and pre-stored in the remote server.

27. The computer readable medium of claim 26, wherein a user having registered the set of retrieval questions is notified if anyone asks for the set of retrieval questions.

28. The computer readable medium of claim 26, further including computer readable instructions encoded thereon for displaying the set of retrieval questions.

29. A client workstation comprising:

a processor;

a display connected to the processor;

a computer memory connected to the processor, the computer memory including:

a viewing program for rendering information received from a server on the display, the display displaying a plurality of entries for entering a plurality of pass phrase answers and an option for requesting a plurality of pass phrase questions corresponding to the plurality of the pass phrase of answers, and

a client program for combining the pass phrase answers to form a single pass phrase,

wherein if the option for requesting the set of the pass phrase questions is chosen, an entry for entering a retrieval answer and an option for requesting a retrieval question corresponding to the retrieval answer is displayed.

30. The client workstation of claim 29, wherein if the option for requesting the retrieval question is chosen, a request is formed and transmitted to the server, which authenticates the request and returns the retrieval question for display if authentication is successful, and if the retrieval answer is entered immediately or entered after the retrieval question is displayed, the validity of the retrieval answer is determined, and if the retrieval answer is determined to be valid, the pass phrase questions are displayed.

31. A computer network comprising:

a client workstation, the client workstation constructing a pass phrase from a plurality of pass phrase answers entered by a user at the client workstation;

a network connected to the client workstation; and

a server connected to the client workstation through the network, the server receiving a request from the client workstation for a plurality of pass phrase questions corresponding to a plurality of pass phrase answers pre-stored in the server, and in response to the request for pass phrase questions, transmitting a request to the client workstation for a retrieval answer corresponding to a retrieval question pre-stored in the server.

32. The computer network of claim 31, wherein the client workstation transmits a request to the server for the retrieval question if the retrieval answer is not entered immediately by the user, the server authenticates the requests and returns the retrieval question to the client workstations for display if authentication is successful.

33. The computer network of claim 21, wherein if the retrieval answer is entered immediately or entered after the retrieval question is displayed, the validity of the retrieval answer is determined, and if the retrieval answer is determined to be valid, the pass phrase questions are displayed.

34. The computer network of claim 31, further comprising a middle server, through which the client workstation and the server transmit requests and requested information to and from each other.